2022 9th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS) | 978-1-6654-7872-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/CFIS54774.2022.9756458

A Dynamic SDN-based Privacy-Preserving Approach for Smart City Using Trust Technique

Jafar A. Alzubi[1], AliAkbar Movassagh[2], Mehdi Gheisari[3], Hamid Esmaeili Najafabadi[4], Aaqif Afzaal Abbasi[5], Yang Liu[6,*], Zhou Pingmei[7], Mahdieh Izadpanahkakhk[8], AmirHossein Pourishaban Najafabadi[9]

[1] Faculty of Engineering, Al-Balqa Applied University, Salt – Jordan (j.zubi@bau.edu.jo)
[2]Department of Medical Physics and Biomedical Engineering, School of Medicine, Tehran University of medical sciences, Tehran, Iran (A.movassagh@gmail.com)
[3]Young Researchers and Elite Club, Parand Branch, Islamic Azad University, Parand, Iran (mehdi.gheisari61@gmail.com)
[4]University of Calgary, Canada (hamid.esmaeili@gmail.com)
[5] Department of Software Engineering, Foundation University, Islamabad 44000, Pakistan (aaqif.afzaal@yahoo.com)
[6]Department of computer science and technology, Harbin Institute of Technology, Shenzhen, China (liu.yang@hit.edu.cn)
[7]Shenzhen BKD company, Shenzhen, China (bkd@bkdlink.com)
[8]DIET department, La Sapienza University, Rome, Italy (izadpanahkakhk@diag.uniroma1.it)
[9]Department of Electrical and Computer Engineering, University of Yazd, Yazd, Iran(amirhosseinpurishaban@gmail.com)

***Abstract*—A smart city is an Internet-based application of things that automates city management with no need for human interference. Exchanging data via devices obviate some challenges in intelligent cities. In a smart city, Internet-of-Things (IoT) devices may detect sensitive data, posing a risk of privacy violation and system harm. We discover that existing solutions are either too expensive or ineffective at limiting unintended disclosure of sensitive data to build a dependable, smart city. The fact that they create static surroundings is the fundamental reason behind this. Software-Defined Networking (SDN) technology has recently evolved to configure the network for performance and monitoring improvement. This study offers a work-in-progress that uses the SDN to protect the privacy of IoT devices by creating a dynamic SDN-based privacy-preserving ecology. The mechanism of the SDN controller performs under the nodes' mutual trust; it chooses various routes from the IoT device to the Cloud space destination dependent on the level of confidence. The packet is re-routed if the SDN controller identifies a device that does not trust its neighbor. Then it instructs the owner to deliver data over a different path. To demonstrate its improved performance, we are currently evaluating it from the perspective of overhead criteria in the future.**

Keywords-Internet of Things; Trust, Smart City; Privacy-Preservation; smart city

I. Introduction

Due to the growing number of inhabitants worldwide by 2050, city management is one of the motivational issues. As predicted, fresh practical solutions to efficiently run cities in duties such as public transit, waste collection, and so on are in high demand [1]. The Internet of Things (IoT) and cloud computing are two developing technologies that have the potential to improve existing city management. A city can address its difficulties more intelligently by combining these two technologies, which is often referred to as a Smart City.

The Internet of Items envisions a connected universe of existing things that can be accessed at any time and from any location. Cloud computing, on the other hand, refers to all of the computer gear and software that a third-party corporation provides to the end-user as a service over the Internet.

Because of the widespread use of IoT, the number of IoT devices integrated into an intelligent city will number in the billions by 2050 according to Gartner's report [2]. The intelligent city market will be worth USD 1.2 trillion by the end of 2020, which is nearly 3 times greater than in 2014 [3]. Within a smart city, IoT sensors drive data to cloud computing not only to provide more in-depth analysis but also to share intelligence alongside other people [4]. An example of an IoT application is a smart house, whereas a traditional home is outfitted with IoT with the goal of improved management. Fig. 1 displays a smart home, which is one of the key components of a smart city.

Figure 1. Example of an old-fashioned intelligent home in a modern city.

As illustrated in Fig. 1, IoT technology in an intelligent city (like intelligent houses), share data with the cloud computing space to make top-quality decision-making [5]. These devices

[*]Corresponding Author: Yang Liu

can be mobile, such as cars, or stationary, such as smartwatches, which stream information straight to the cloud.

More data, in general, means more opportunities to provide high-level services. However, it also brings up a significant challenging issue, which is privacy protection since that some smart city device may produce sensitive data. Malicious behaviors may create trouble and errors in the system if sensitive data is released involuntarily. As a result, while they collaborate to provide high-level services, these data should be securely protected. If the privacy concern is addressed, citizens will be more inclined to use the Internet of Things-based smart city. There are three sorts of sensitive data that should not be accidentally published:

1) Personal information: information that allows an individual or an IoT device to be directly authenticated, such as a person's name, the number of people alive in a large building, a low brake oil level in an autonomous vehicle, a social security number, and so on.

2) Semi-sensitive information, such as wages and medical conditions.

3) Information with a quasi-identifier: We must avoid unintentional publication of this type of data because by integrating and merging sensed data with information collected from external sources, we may distinguish the data of a given IoT device or individual. such as a public-voting registration database, a database of IoT device locations, a database of hospital registrations, and so on. In other words, a specific IoT device can be identified by combining the provided data with external databases.

Considering the above, we should provide methods to avoid sensitive data from being accidentally disclosed. Otherwise, there is a good chance it will be abused by adversaries attempting to physically or cyber-attack the system. Assume an IoT device detects the number of individuals alive in a significant building. This information must not be accidentally released since adversaries can alert a third party, who can then analyze the information and launch physical or virtual attacks on the building.

We discovered that present solutions could not provide an effective environment because they are either too expensive [6], [4], or lack the required performance from a privacy-preserving standpoint [7]. Finding a middle ground between these two research objectives is a big difficulty in creating an efficient smart city where inhabitants can trust smart city technologies while knowing that sensitive data will not be accidentally released.

Meanwhile, the Software-Defined Networking approach has become a popular networking model for dividing the data plane and the control plane [8]. This split results in a network that is flexible to administer. It provides a centralized view of a full network and makes network management more efficient. In other words, it enables network equipment administration from a single centralized controller, which is impossible to achieve with the classic Simple Network Management Protocol (SNMP). In an SDN environment, one of the key advantages is the ability to control data traffic. Network setup and maintenance will be done in a more convenient manner using SDN [9-15].

In this paper, we offer a privacy-preserving approach for IoT devices integrated into a smart city to address some challenges between current studies., where the packets are through the SDN controller, data is delivered to the cloud computing area. They transmit their data to the cloud computing space for easier data exchange and high-level decision-making since it delivers on-demand computer system resources [10, 16-17, 20-28]. If neighbors do not trust each other, this is accomplished by rerouting data packets.

We intend to analyze the proposed method and compare it to the state-of-the-art after publishing this work-in-progress. We will evaluate it based on many parameters, including the quantity of privacy-preserving degree, computing cost, latency, and communication overhead. In a nutshell, the proposed technique entails the stages below:

1) To operate the network flexibly, we equip contemporary smart cities with the SDN paradigm.

2) We present a solution for preserving the privacy of IoT devices on top of the outfitted environment. If the IoT device's trust in its next neighbor is less than 50%, the SDN controller instructs it to reroute its sensitive data. This schema is based on a guess. To locate the best deal, more research is required. As a result, if the device generates sensitive data, the SDN controller is in charge of routing the data from the IoT device to itself. The controller does not allow data to be redirected from the established path if a node's trust in its neighbor is less than 50%. Rather, it instructs the IoT device to send data over a new route defined by the SDN controller. On the other hand, if the trust level exceeds 50%, sensitive data will be sent via a predetermined channel. Finally, the SDN controller transfers the data to Cloud Computing for additional analysis.

3)We will assess our proposed method from multiple perspectives, including privacy-preserving degree and penetration rate, overhead, and latency, to demonstrate its improved performance over current studies. We will demonstrate that, although adding more overhead to the IoT-based smart city, our technology effectively protects the privacy of IoT devices. If it can be widely employed in smart cities.

This is how the paper is structured. The second section discusses the literature that is relevant to this topic. The proposed approach is then thoroughly explained in Section III. Section V brings the paper to a close and makes recommendations for further research.

II. LITERATURE REVIEW

Several current research trends aim to use the SDN paradigm to protect the privacy of IoT devices in a smart city. The general concept is that data is sent to the cloud computing space for additional analysis and command execution. In [11], the authors suggested a paradigm for providing end-to-end security and privacy in 5G-enabled vehicle networks. Their suggested system used the SDN paradigm to simplify network management while achieving optimal network connectivity. It consists of two modules: the first is an authentication protocol that uses elliptic curve cryptography (ECC) for mutual authentication between cluster heads (CH) and certificate authorities (CA) in automotive contexts using the SDN [12, 25-32]. The Intrusion Detection module is the second designed module, and it detects potential intrusions in the system. The module has minimal computational complexity, according to the researchers. They used three simulators to fully exploit the suggested framework's potential benefits (e.g., NS3, SUMO, and SPAN). The first module was evaluated based on its security features. The detection rate, false-positive rate, accuracy, detection time, and communication overhead were all included in the second module evaluation compared with the state of the art.

Using the SDN paradigm, the authors of [5] devised a solution for safeguarding the privacy of IoT devices in a smart city. Their technology is context-aware, allowing users to react to their surroundings based on their current situation. First, they installed the SDN paradigm in the smart city. Then they implement a privacy-preserving mechanism in which the device generates sensitive data and separates it into two portions, each comprising 70% and 30% of the original data. The first division is then sent to the SDN controller through the most secure path. The remaining data is sent to the SDN controller via a built virtual private network (VPN). The controller then aggregates the device's data. Finally, it sends the compiled data to the smart city cloud for further analysis and command execution. Several evaluation measures, including accuracy, penetration time, and overload, were used to assess their suggested technique. They also contrasted their answer to what was currently available. They discovered that their method is more effective at preventing unintentional sensitive data disclosure. Simultaneously, it adds to the smart city's workload.

Meantime, [13] inspires us, even though the authors did not use the SDN paradigm. They presented a lightweight privacy-preserving data aggregation (PDA) approach for the fog-computing-enabled IoT environment. To encrypt the data flow, they used the homomorphic Paillier cryptosystem. They also used the Chinese remainder theorem (CRT) to combine data from a variety of IoT devices [14]. To provide a more efficient solution, they also used a one-way hash chain function to filter injected bogus data at the network edge-level forging and had more efficient authentication of IoT devices [15]. They also used differential privacy-preserving (DP) as a supplement to create more effective privacy-preserving [16]. Furthermore, their technology is light enough to be used in real-time demanding situations. Aside from the benefits indicated, the PDA has a disadvantage in that it is not adaptable or agile.

Similarly, the authors of [2] devised a privacy-preserving approach for the IoT using the SDN paradigm. They installed software on the SDN controller, allowing it to govern IoT device data flow. To begin, the SDN controller divides IoT devices into numerous categories. Based on their associated class label, it then selects whether to encrypt, aggregate, or transfer their data to the SDN controller through an established VPN. Although the authors evaluated their proposed strategy based on the amount of overhead, this is insufficient to determine if their solution can effectively protect the privacy of IoT devices. Furthermore, the approach they provide is not context-aware.

In [8], the authors built on their earlier work and suggested a way for increasing the privacy of IoT-based smart cities with SDNs. They imagined a situation in which five smart buildings generate sensitive data and want to send it to a cloud computing environment for further study [17]. A solution was presented to maintain the privacy of smart buildings by splitting them into two sub-categories on top of the equipped smart city. An encryption mechanism is used if the smart building is classed in the first category. Otherwise, the data is split into two portions and sent to the SDN controller over two distinct routes.

They evaluated the amount of overhead and compared it to the time it takes IoT devices to deliver data straight to the cloud computing area to evaluate the proposed method. Although this strategy is cost-effective for many IoT devices, the solution's performance has not been evaluated in terms of privacy protection. Using zonal architecture to shield devices and data using multiple layers or zones is also a method to ensure privacy. [18]. And with deep learning and AI coming into play [19], privacy is of utmost importance. Furthermore, encryption is used as a preventative step to conceal crucial data that can be omitted [20].

III. PROPOSED METHOD

A. Assumptions

We consider IoT devices already know whether the sensitivity of gathered data. Furthermore, specialists have already entered safe routes from an IoT device to the SDN controller into a database. As previously stated, the SDN controller knows the trust relationship between nodes via a database that is considered static in this paper.

B. Procedure

This section proposes a unique approach for improving the efficiency and privacy of IoT devices in a smart city. It includes the principle of dynamically preserving the privacy of IoT devices based on the degree of trust among nodes. Our scenario utilizes the same database as [5]. So far, we've got a laptop, a smartwatch, a smart building, a smartphone, a garbage can, and an autonomous vehicle. They are supplying numerical information. They intend to send their data to the Cloud. They have the SDN paradigm installed. As a result, IoT devices send data to an SDN controller first, then to the Cloud. As mentioned in the previous section, the SDN controller has the dataset of trust amounts between nodes. The SDN controller verifies the trust amount when an IoT device wants to send sensitive data. If the trust level is less than the threshold=0.5, the IoT device is instructed to transfer sensitive data through a different random route. If not, it follows the predetermined path and transfers the data to its neighbor. The approach for the proposed solution in this paper is shown in the following.

Algorithm I. Proposed Privacy-preserving algorithm

```
Input: X= The sensed data
for all IoT devices do
    if X= Sensitive data then
      The SDN controller specifies the first secure
       route of the database from the IoT device to
       itself;
    for All Middle Nodes do
        T=The amount of trust among nodes;
        if T is less than 50% then
            SDN controller specifies a new random
              route;
Output: NULL
```

IV. ANALYSIS AND RESULTS

This section evaluates our proposed method from the overhead point of view. In other words, in this section, we determine how much strain it places on IoT devices or how much overhead the system should tolerate from the computational cost perspective.

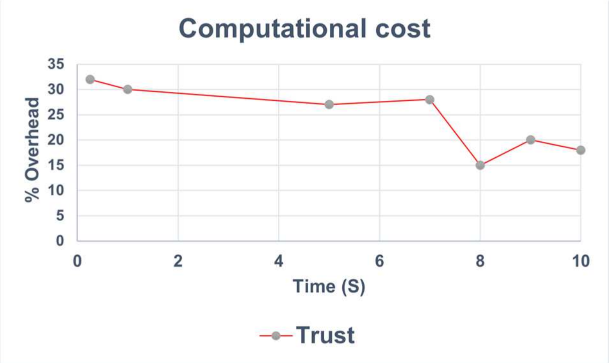

Figure 2. The amount of overhead in terms of time

As Figure 2 shows, our solution imposes, in the beginning, around 35% overhead. This amount decreases during the steady phase.

CONCLUSION

In this ongoing research, we first installed the SDN paradigm in a smart home. Then, on top of the SDN controller, we installed software to manage data flow flexibly based on the amount of trust among nodes. If the level of trust is less than 50%, it instructs the IoT device to reroute its data and send it via a different secure route. However, if the percentage is greater than 50%, the device sends sensitive data via the predefined route. To complete this research, we intend to evaluate it from a variety of perspectives, including privacy preservation, overhead, latency, and so on. In the future, we want to expand this approach and examine it from many angles to see if it outperforms current studies.

ACKNOWLEDGMENT

This work is supported by the Shenzhen Basic Research (General Project)(No. JCYJ20190806142601687) and Shenzhen Stable Supporting Program (General Project) (No. GXWD20201230155427003-20200821160539001).

REFERENCES

[1] R. Du, P. Santi, M. Xiao, A. V. Vasilakos, and C. Fischione, “The sensible city: A survey on the deployment and management for smart city monitoring,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp.1533–1560, 2018.

[2] M. Gheisari, et al, “A method for privacy-preserving in IoT-SDN integration environment,” in *2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications* (ISPA/IUCC/BDCloud/SocialCom/SustainCom). IEEE, 2018, pp. 895–902.

[3] P. Neirotti, A. De Marco, A. C. Cagliano, G. Mangano, and F. Scorrano, “Current trends in smart city initiatives: Some stylised facts,” *Cities*, vol. 38, pp. 25–36, 2014.

[4] M. Gheisari, et al, “Eca: an edge computing architecture for privacy-preserving in IoT-based smart city,” *IEEE Access*, vol. 7, pp. 155 779–155 786, 2019.

[5] M. Gheisari, G. Wang, W. Z. Khan, and C. Fernández-Campusano, “A context-aware privacy-preserving method for IoT-based smart city using Software Defined Networking,” *Computers & Security*, vol. 87, p. 101470, 2019.

[6] P. G. V. Naranjo, Z. Pooranian, M. Shojafar, M. Conti, and R. Buyya, “Focan: A fog-supported smart city network architecture for management of applications in the internet of everything environments,” *Journal of parallel and distributed computing*, vol. 132, pp. 274–283, 2019.

[7] M. S. Rahman, I. Khalil, M. Atiquzzaman, and X. Yi, “Towards privacy preserving ai based composition framework in edge networks using fully homomorphic encryption,” *Engineering Applications of Artificial Intelligence*, vol. 94, p. 103737, 2020.

[8] M. Gheisari, G. Wang, S. Chen, and H. Ghorbani, “Iot-sdnpp: A method for privacy-preserving in smart city with software defined networking,” in *International Conference on Algorithms and Architectures for Parallel Processing*. Springer, 2018, pp. 303–312.

[9] W. Braun and M. Menth, “Software-defined networking using openflow: Protocols, applications and architectural design choices,” *Future Internet*, vol. 6, no. 2, pp. 302–336, 2014.

[10] T.-S. Chou, “Security threats on cloud computing vulnerabilities,” *International Journal of Computer Science & Information Technology*, vol. 5, no. 3, p. 79, 2013.

[11] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, “Sdn-based secure and privacy-preserving scheme for vehicular networks: A 5g perspective,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 8421–8434, 2019.

[12] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, “Nanoecc: Testing the limits of elliptic curve cryptography in sensor networks,” in *European conference on Wireless Sensor Networks*. Springer, 2008, pp.305–320.

[13] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, “A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot,” *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[14] M. Jafari, J. Wang, et al, “Automatic text summarization using fuzzy inference,” in *2016 22nd International Conference on Automation and Computing (ICAC)*. IEEE, 2016, pp. 256–260.

[15] M. Gheisari, “The effectiveness of schema therapy integrated with neurological rehabilitation methods to improve executive functions in patients with chronic depression,” *Health Science Journal*, vol. 10, no. 4, p. 1, 2016.

[16] E. GhadakSaz, M. R. Amini, P. Porkar, and M. Gheisari, “Design, implement and compare two proposed sensor data storages named semhd and ssw,” From Editor in Chief, p. 78, 2012.

[17] Q. Liu, G. Wang, X. Liu, T. Peng, and J. Wu, “Achieving reliable and secure services in cloud computing environments,” *Computers & Electrical Engineering*, vol. 59, pp. 153–164, 2017.

[18] A. J. Moshayedi, A. S. Roy, L. Liao and S. Li, "Raspberry Pi SCADA Zonal based System for Agricultural Plant Monitoring," 2019 6th International Conference on Information Science and Control Engineering (ICISCE), 2019, pp. 427-433, doi: 10.1109/ICISCE48695.2019.00092.

[19] Moshayedi, A. J., Roy, A. S., Kolahdooz, A., & Shuxin, Y. (2022). Deep Learning Application Pros and Cons Over Algorithm. EAI Endorsed

Transactions on AI and Robotics, 1, 1-13.

[20] S. Yu, G. Wang, and W. Zhou, “Modeling malicious activities in cyber space,” *IEEE network*, vol. 29, no. 6, pp. 83–87, 2015.

[21] Ashourian, Mohsen, et al. "An Improved Node Scheduling Scheme for Resilient Packet Ring Network." *Majlesi Journal of Electrical Engineering* 9.2 (2015): 43

[22] Fakhimi, Esmaeil, et al. "Design Two Sensor Data Storages." International Conference on Advanced Computer Theory and Engineering, 4th (ICACTE 2011). *ASME Press*, 2011.

[23] Mehdi Gheisari, et al, A Method for Privacy-preserving in IoT-SDN Integration Environment, *16th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2018),* 11-13 Dec. 2018, Melbourne, Australia

[24] M. Gheisari et al., "A Survey on Clustering Algorithms in Wireless Sensor Networks: Challenges, Research, and Trends," *2020 International Computer Symposium (ICS)*, Tainan, Taiwan, 2020, pp. 294-299

[25] Rezaeiye, Payam Porkar, et al. "Agent programming with object oriented (C++)." *Electrical, Computer and Communication Technologies (ICECCT),* 2017 Second International Conference on. IEEE, 2017.

[26] Gheisari, Mehdi, et al. "MAPP: A Modular Arithmetic Algorithm for Privacy Preserving in IoT." *Ubiquitous Computing and Communications (ISPA/IUCC), 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on. IEEE*, 2017.

[27] Movassagh, *et al.* Artificial neural networks training algorithm integrating invasive weed optimization with differential evolutionary model. *J Ambient Intell Human Comput* (2021).

[28] Natarajan, Y., et al.: An IoT and machine learning-based routing protocol for reconfigurable engineering application. *IET Commun*. 00, 1– 12 (2021).

[29] K. A. Raza, A. Asheralieva, et al , "A Novel Forwarding and Caching Scheme for Information-Centric Software-Defined Networks," *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, 2021, pp. 1-8, doi: 10.1109/ISNCC52172.2021.9615667.

[30] Yogesh Kumar, Apeksha Koul, et al , "Heart Failure Detection Using Quantum-Enhanced Machine Learning and Traditional Machine Learning Techniques for Internet of Artificially Intelligent Medical Things", *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 1616725, 16 pages, 2021.

[31] Li, Lintao, et al. "Research on TCP Performance Model and Transport Agent Architecture in Broadband Wireless Network." *Scalable Computing: Practice and Experience* 22.2 (2021): 193-201.

[32] Mangla, Monika, et al. "A Proposed Framework for Autonomic Resource Management in Cloud Computing Environment." *Autonomic Computing in Cloud Resource Management in Industry 4.0.* Springer, Cham, 2021. 177-193.